Version : **2022.01**

Updated: 2022/11/21 09:34

Topic 207: Domain Name Server

Contenu du Module

Présentation

Le principe du DNS est basé sur l'équivalence entre un **FQDN** (Fully Qualified Domain Name) et une adresse IP. Les humains retiennent plus facilement des noms tels www.i2tch.com, tandis que les ordinateurs utilisent des chiffres.

Le **DNS** (Domain Name Service) est né peut après l'introduction des FQDN en 1981.

Lorsque un ordinateur souhaite communiquer avec un autre par le biais de son nom, par exemple avec www.i2tch.com, il envoie une requête à un server DNS. Si le serveur DNS a connaissance de la correspondance entre le nom demandé et le numéro IP, il répond directement. Si ce n'est pas le cas, il démarre un processus de **Recursive Lookup**.

Ce processus tente d'identifier le serveur de domaine responsable pour le **SLD** (Second Level Domain) afin de lui passer la requête. Dans notre exemple, il tenterait d'identifier le serveur de domaine responsable de **i2tch.com**.

Si cette tentative échoue, le serveur DNS cherche le serveur de domaine pour le **TLD** (Top Level Domain) dans son cache afin de lui demander l'adresse du serveur responsable du SLD. Dans notre cas il tenterait trouver l'enregistrement pour le serveur de domaine responsable de **.com**

Si cette recherche échoue, le serveur s'adresse à un **Root Name Server** dont il y en a peu. Si le Root Name Server ne peut pas répondre, le serveur DNS renvoie une erreur à la machine ayant formulé la demande.

Le serveur DNS sert à faire la résolution de noms. Autrement dit de traduire une adresse Internet telle **www.i2tch.com** en **numéro IP**.

LAB #1 - Installation

1.1 - Préparation à l'Installation

Le serveur DNS nécessite à ce que la machine sur laquelle il est installé possède un FQDN et une adresse IP fixe. Il est également important à noter que le service de bind ne démarrera **pas** dans le cas où le fichier **/etc/hosts** comporte une anomalie. Trois étapes préparatoires sont donc nécessaires :

- Modification de l'adresse IP de la machine en adresse IP fixe

- Définition d'un nom FQDN (Fully Qualified Domain Name)
- Vérification du fichier /etc/hosts

Afin d'étudier ce dernier cas, nous prenons en tant qu'exemple la machine suivante :

- **FQDN** - centos7.fenestros.loc
- **Adresse IP** - 10.0.2.51

Modifiez votre fichier /etc/hosts :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
10.0.2.51       centos7.fenestros.loc
127.0.0.1       localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
```

> **Important** : Il est important de noter que la configuration du serveur DNS dépend du nom de votre machine. Dans le cas où vous changeriez ce nom, vous devez re-configurer votre serveur DNS en éditant les fichiers de configuration directement.

1.2 - Installation de bind

Pour installer le serveur DNS, utilisez la commande **yum**:

```
[root@centos7 ~]# yum install bind
```

Activez le service **named** du paquet **bind** :

```
[root@centos7 ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
```

```
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@centos7 ~]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to
/usr/lib/systemd/system/named.service.
[root@centos7 ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
```

Important : NE DEMARREZ PAS le service named.

LAB #2 - Les fichiers de configuration

Six fichiers doivent être modifiés pour que bind fonctionne correctement :

- /var/named/named.ca
- /etc/named.conf
- /var/named/named.loopback
- /var/named/named.localhost
- /var/named/data/db.2.0.10.hosts
- /var/named/data/db.fenestros.loc.hosts

2.1 - named.ca

Ce fichier doit se trouver dans /var/named.

Le fichier **named.ca** a besoin d'être mis à jour en utilisant la commande **dig** :

```
[root@centos7 ~]# dig +tcp @A.ROOT-SERVERS.NET > /var/named/named.ca

[root@centos7 ~]# cat /var/named/named.ca

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10 <<>> +tcp @A.ROOT-SERVERS.NET
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4806
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      e.root-servers.net.
.                       518400  IN      NS      h.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      i.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
.                       518400  IN      NS      d.root-servers.net.
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      b.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      k.root-servers.net.
.                       518400  IN      NS      g.root-servers.net.
.                       518400  IN      NS      m.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.

;; ADDITIONAL SECTION:
e.root-servers.net.     518400  IN      A       192.203.230.10
```

```
e.root-servers.net.     518400  IN      AAAA    2001:500:a8::e
h.root-servers.net.     518400  IN      A       198.97.190.53
h.root-servers.net.     518400  IN      AAAA    2001:500:1::53
l.root-servers.net.     518400  IN      A       199.7.83.42
l.root-servers.net.     518400  IN      AAAA    2001:500:9f::42
i.root-servers.net.     518400  IN      A       192.36.148.17
i.root-servers.net.     518400  IN      AAAA    2001:7fe::53
a.root-servers.net.     518400  IN      A       198.41.0.4
a.root-servers.net.     518400  IN      AAAA    2001:503:ba3e::2:30
d.root-servers.net.     518400  IN      A       199.7.91.13
d.root-servers.net.     518400  IN      AAAA    2001:500:2d::d
c.root-servers.net.     518400  IN      A       192.33.4.12
c.root-servers.net.     518400  IN      AAAA    2001:500:2::c
b.root-servers.net.     518400  IN      A       199.9.14.201
b.root-servers.net.     518400  IN      AAAA    2001:500:200::b
j.root-servers.net.     518400  IN      A       192.58.128.30
j.root-servers.net.     518400  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     518400  IN      A       193.0.14.129
k.root-servers.net.     518400  IN      AAAA    2001:7fd::1
g.root-servers.net.     518400  IN      A       192.112.36.4
g.root-servers.net.     518400  IN      AAAA    2001:500:12::d0d
m.root-servers.net.     518400  IN      A       202.12.27.33
m.root-servers.net.     518400  IN      AAAA    2001:dc3::35
f.root-servers.net.     518400  IN      A       192.5.5.241
f.root-servers.net.     518400  IN      AAAA    2001:500:2f::f

;; Query time: 2 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Nov 01 16:59:11 CET 2022
;; MSG SIZE  rcvd: 811
```

2.2 - named.conf

Le fichier de configuration principal du serveur DNS Bind est **/etc/named.conf** :

```
[root@centos7 ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
```

```
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Important : Notez que pour désactiver les requêtes récursives, il convient de passer la valeur de la directive **recursion** à no : recursion no;

Dans ce fichier on trouve des sections ayant la forme suivante :

```
section {
   variable1  valeur1;
   variable2  valeur2;
};
```

Il existe différentes sections dont une des plus importantes est **options**. C'est dans cette section que nous définissons les options globales:

```
...
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; };

        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        bindkeys-file "/etc/named.root.key";
```

```
        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};
...
```

Notons certaines directives. D'abord nous définissons le chemin des fichiers des **zones**:

```
directory "/var/named";
```

Afin de limiter les machines qui peuvent et qui ne peuvent pas utiliser notre DNS, nous utilisons la valeur “allow-query”. Dans notre cas les requêtes sont permises en provenance uniquement du localhost :

```
allow-query { localhost; };
```

Modifiez donc la section **options** de votre fichier **/etc/named.conf** ainsi :

```
[root@centos7 ~]# vi /etc/named.conf
[root@centos7 ~]# cat /etc/named.conf
...
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query {
                localhost;
                10.0.2.0/24;
        };
```

```
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        bindkeys-file "/etc/named.root.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};
...
```

Important - Dans l'exemple ci-dessus nous autorisons toutes les machines de notre réseau, ainsi que la machine locale à utiliser le DNS. Notez aussi que pour limiter les connexions à partir de serveurs DNS esclaves, il convient d'ajouter une directive **allow-transfer**.

Dernièrement, il est possible de créer des ACLs qui peuvent être utilisés avec la directive **allow-query** :

```
        acl mycompany {
            10.0.2.0/24; 192.168.56.0/24;
        };

        options {
            allow-query { mycompany; };
        };
```

2.3 - named.rfc1912.zones

Dans le fichier **/etc/named.conf** vous pouvez constater la présence d'une directive **include “/etc/named.rfc1912.zones”;**.

Consultez ce fichier :

```
[root@centos7 ~]# cat /etc/named.rfc1912.zones
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
```

```
        file "named.loopback";
        allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.empty";
        allow-update { none; };
};
```

La Valeur Type

Maintenant, étudions les sections de zones. La valeur “type” peut prendre plusieurs valeurs:

- **master**
  - Ce type définit le serveur DNS comme serveur maître ayant **autorité** sur la zone concernée.
- **slave**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée. Ceci implique que la zone est une réplication d'une zone maître. Un type de zone esclave contiendra aussi une directive **masters** indiquant les adresses IP des serveurs DNS maîtres.
- **stub**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée mais uniquement pour les **enregistrements** de type **NS**.
- **forward**
  - Ce type définit le serveur DNS comme serveur de transit pour la zone concernée. Ceci implique que toute requête est re-transmise vers un autre serveur.
- **hint**
  - Ce type définit la zone concernée comme une zone racine. Ceci implique que lors du démarrage du serveur, cette zone est utilisée pour récupérer les adresses des serveurs DNS racine.

La valeur “notify” est utilisée pour indiquer si non (no) ou oui (yes) les autres serveurs DNS sont informés de changements dans la zone.

La Valeur File

La deuxième directive dans une section de zone comporte la valeur **file**. Il indique l'emplacement du fichier de zone.

Exemples

Chaque section de zone, à l'exception de la zone “.” est associée avec une section de zone inversée.

La zone “.” est configurée dans le fichier **/etc/named.conf** :

```
...
zone "." IN {
    type hint;
    file "named.ca";
};
...
```

La section de zone fait correspondre un nom avec une adresse IP tandis que la section de zone inversée fait l'inverse. La section inversée a un nom d'un syntaxe spécifique :

```
adresse_réseau_inversée.in-addr.arpa.
```

Par exemple dans le fichier ci-dessus nous trouvons les cinq sections suivantes :

```
...
zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
```

```
};

zone "localhost" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.empty";
        allow-update { none; };
};
```

Important - Notez la présence de deux sections inversées, respectivement pour IPv4 et IPv6. Dans la suite de cette leçon, nous allons nous concentrer sur IPv4.

Afin de configurer notre serveur correctement donc, il est nécessaire d'ajouter à ce fichier deux sections supplémentaires.

La zone correspondant à notre domaine, ici appelée “fenestros.loc”. Celle-ci fait correspondre le nom de la machine avec son adresse IP:

```
...
zone "fenestros.loc" {
    type master;
    file "data/db.fenestros.loc.hosts";
    forwarders { };
};
...
```

La zone à notre domaine mais dans le sens inverse. A savoir le fichier **db.2.0.10.hosts** qui fait correspondre notre adresse IP avec le nom de la machine.

```
...
zone "2.0.10.in-addr.arpa" {
    type master;
    file "data/db.2.0.10.hosts";
    forwarders { };
};
...
```

Ajoutez donc ces deux sections au fichier **/etc/named.rfc1912.zones** :

```
[root@centos7 ~]# vi /etc/named.rfc1912.zones

[root@centos7 ~]# cat /etc/named.rfc1912.zones
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
```

```
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.empty";
        allow-update { none; };
};
```

```
zone "fenestros.loc" {
    type master;
    file "data/db.fenestros.loc.hosts";
    forwarders { };
};

zone "2.0.10.in-addr.arpa" {
    type master;
    file "data/db.2.0.10.hosts";
    forwarders { };
};
```

2.4 - Les fichiers de zone

La fichiers de zone sont composées de lignes d'une forme:

nom	TTL	classe	type	donnée

où

- **nom**
  - Le nom DNS.
- **TTL**
  - La durée de vie en cache de cet enregistrement.
- **classe**
  - Le réseau de transport utilisé. Dans notre cas, Internet. La valeur est donc IN.
- **type**
  - Le type d'enregistrement:
    - SOA - Start of Authority - se trouve au début du fichier et contient des informations générales
    - NS - Name Server - le nom du serveur de nom
    - A - Address IPv4 - indique une résolution de nom vers une adresse IP. Ne se trouve que dans les fichiers **.hosts**
    - AAAA - Address IPv6 - indique une résolution de nom vers une adresse IP. Ne se trouve que dans les fichiers **.hosts**
    - PTR - PoinTeR - indique une résolution d'une adresse IP vers un nom. Ne se trouve que dans les fichiers inversés.

        - MX - Mail eXchange - le nom d'un serveur de mail.
        - CNAME - Canonical Name - un alias d'une machine.
        - HINFO - Hardware Info - fournit des informations sur le matériel de la machine
        - TXT - Un enregistrement contenant des informations textuelles pour des sources extérieures à votre domaine, par exemple :
            - Vérification de la propriété du domaine
            - Implémentation du **Sender Policy Framework** (SPF)
            - Enregistrements **DomainKeys Identified Mail** (DKIM) pour vérifier l'expéditeur des messages électroniques
            - **Zero-configuration networking DNS-based service discovery**
            - Politiques de **Domain-based Message Authentication, Reporting and Conformance**.
- **donnée**
    - La donnée de la ressource:
        - Une adresse IP pour un enregistrement de type A
        - Un nom de machine pour un eregistrement de type PTR

Le fichier db.fenestros.loc.hosts

Ce fichier doit être créé dans /var/named/data. Il est le fichier qui définit la correspondance du nom de la machine **centos7.fenestros.loc** avec son numéro IP, à savoir le **10.0.2.51**. On définit dans ce fichier les machines qui doivent être appelées par leur nom :

```
[root@centos7 ~]# vi /var/named/data/db.fenestros.loc.hosts
[root@centos7 ~]# cat /var/named/data/db.fenestros.loc.hosts
$TTL 3D
@       IN     SOA     centos7.fenestros.loc. root.centos7.fenestros.loc. (
               2022110101       ; Serial
               8H   ; Refresh
               2H   ; Retry
               4W  ; Expire
               1D)  ; Minimum TTL
               IN      NS      centos7.fenestros.loc.
localhost                   A              127.0.0.1
dnsmaster                   IN      CNAME  centos7.fenestros.loc.
centos7.fenestros.loc.       IN      A      10.0.2.51
```

```
ftp IN CNAME centos7.fenestros.loc.
www IN CNAME centos7.fenestros.loc.
mail IN CNAME centos7.fenestros.loc.
news IN CNAME centos7.fenestros.loc.
```

La première ligne de ce fichier commence par une ligne semblable à celle-ci:

```
$TTL 3D
```

Cette ligne indique aux autres serveurs DNS pendant combien de temps ils doivent garder en cache les enregistrements de cette zone. La durée peut s'exprimer en jours (**D**), en heures (**H**) ou en secondes (**S**).

La deuxième ligne définit une **classe IN**ternet, un **SOA** (Start Of Authority), le nom du serveur primaire et l'adresse de l'administrateur de mail :

```
@       IN     SOA     centos7.fenestros.loc. root.centos7.fenestros.loc. (
```

> **Important** - Notez le point à la fin de chaque nom de domaine. Notez bien le remplacement du caractère @ dans l'adresse email de l'administrateur de mail par le caractère “.”

Le caractère **@** au début de la ligne corréspond au nom de la zone et est une abréviation pour le nom de la zone décrit par le fichier de la zone, soit dans ce cas db.**fenestros.loc**.hosts, et présent dans le fichier /etc/named.conf :

```
...
zone "fenestros.loc" {
      type master;
      file "data/db.fenestros.loc.hosts";
      forwarders { };
};
...
```

Le numéro de série doit être modifié chaque fois que le fichier soit changé. Il faut noter que dans le cas de plusieurs changements dans la même journée il est nécessaire d'incrémenter les deux derniers chiffres du numéro de série. Par exemple, dans le cas de deux changements en date du 01/11/2022, le premier fichier comportera une ligne Serial avec la valeur 2022110101 tandis que le deuxième changement comportera le numéro de série 2022110102 :

```
       2022110101       ; Serial
```

La ligne suivante indique le temps de rafraîchissement, soit 8 heures. Ce temps correspond à la durée entre les mises à jour d'un autre serveur :

```
       8H ; Refresh
```

La ligne suivante indique le temps entre de nouveaux essaies de mise à jour d'un autre serveur dans le cas où la durée du Refresh a été dépassée :

```
       2H ; Retry
```

La ligne suivante indique le temps d'expiration, c'est-à-dire la durée d'autorité de l'enregistrement. Cette directive est utilisée seulement par un serveur esclave :

```
       4W ; Expire
```

La ligne suivante indique le temps minimum pour la valeur TTL, soit un jour:

```
       1D) ; Minimum TTL
```

Cette ligne identifie notre serveur de noms :

```
IN NS centos7.fenestros.loc.
```

Dans le cas où notre serveur était également un serveur mail. Nous trouverions aussi une entrée du type SMTP (MX) :

```
IN MX 10 mail.fenestros.loc.
```

Ci-dessous on définit avec une entrée du type A, les machines que l'on souhaite appeler par leur nom, à savoir **centos.fenestros.loc** et **localhost** :

```
localhost                   A             127.0.0.1
centos7.fenestros.loc.      IN      A     10.0.2.51
```

Ci-dessous on définit des **Alias** avec des entrées du type CNAME. Les alias servent à identifier une machine.

```
dnsmaster                   IN      CNAME  centos7.fenestros.loc.
```

Nous pourrions aussi trouver ici des entrées telles:

```
ftp IN CNAME centos7.fenestros.loc.
www IN CNAME centos7.fenestros.loc.
mail IN CNAME centos7.fenestros.loc.
news IN CNAME centos7.fenestros.loc.
```

Le fichier db.2.0.10.hosts

Ce fichier doit être créé dans /var/named/data. Il est le fichier qui définit la correspondance de l'adresse IP de la machine en utilisant un Pointer (PTR), à savoir le **10.0.2.51** avec le nom **centos7.fenestros.loc**. Le chiffre **51** dans la dernière ligne correspond au 10.0.2.**51**:

```
[root@centos7 ~]# vi /var/named/data/db.2.0.10.hosts

[root@centos7 ~]# cat /var/named/data/db.2.0.10.hosts
$TTL 3D
@       IN      SOA     centos7.fenestros.loc.        centos7.fenestros.loc. (
                2022110101 ; Serial
                10800   ; Refresh
                3600    ; Retry
                604800  ; Expire
                86400) ; Minimum TTL
                NS      centos7.fenestros.loc.
51       IN      PTR     centos7.fenestros.loc.
```

Modifiez maintenant les permissions sur les fichiers de configuration :

```
[root@centos7 ~]# chmod g+w /var/named/data/*

[root@centos7 ~]# ls -l /var/named/data/*
-rw-rw-r--. 1 root root 355 Nov  1 17:29 /var/named/data/db.2.0.10.hosts
-rw-rw-r--. 1 root root 619 Nov  1 17:22 /var/named/data/db.fenestros.loc.hosts
```

2.5 - Tester le serveur DNS

Modifiez maintenant le fichier **/etc/resolv.conf** afin d'utiliser votre propre serveur DNS :

```
[root@centos7 ~]# nmcli c mod ip_fixe +ipv4.dns 127.0.0.1

[root@centos7 ~]# nmcli c mod ip_fixe -ipv4.dns 8.8.8.8

[root@centos7 ~]# nmcli c up ip_fixe
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)

[root@centos7 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search fenestros.loc
nameserver 127.0.0.1
```

Dernièrement, démarrez le service named :

```
[root@centos7 ~]# systemctl start named
[root@centos7 ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2022-11-01 17:41:33 CET; 3s ago
  Process: 24441 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
```

```
  Process: 24439 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-
checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 24443 (named)
   CGroup: /system.slice/named.service
           └─24443 /usr/sbin/named -u named -c /etc/named.conf

Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './DNSKEY/IN':
2001:503:ba3e::2:30#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './NS/IN':
2001:503:ba3e::2:30#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './DNSKEY/IN':
2001:500:1::53#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './DNSKEY/IN':
2001:500:200::b#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './NS/IN': 2001:500:200::b#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './DNSKEY/IN':
2001:500:a8::e#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Nov 01 17:41:33 centos7.fenestros.loc named[24443]: managed-keys-zone: Key 20326 for zone . acceptance timer
complete: key now trusted
Nov 01 17:41:34 centos7.fenestros.loc named[24443]: resolver priming query complete
```

Testez maintenant votre serveur :

```
[root@centos7 ~]# dig www.i2tch.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10 <<>> www.i2tch.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48329
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.i2tch.com.                 IN      A

;; ANSWER SECTION:
www.i2tch.com.          3551    IN      A       51.68.204.226

;; AUTHORITY SECTION:
i2tch.com.              172751  IN      NS      ns1026.ui-dns.com.
i2tch.com.              172751  IN      NS      ns1051.ui-dns.de.
i2tch.com.              172751  IN      NS      ns1036.ui-dns.org.
i2tch.com.              172751  IN      NS      ns1051.ui-dns.biz.

;; ADDITIONAL SECTION:
ns1026.ui-dns.com.      172751  IN      A       217.160.82.26
ns1026.ui-dns.com.      172751  IN      AAAA    2001:8d8:fe:53:0:d9a0:521a:100

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 01 17:42:27 CET 2022
;; MSG SIZE  rcvd: 222
```

```
[root@centos7 ~]# dig centos7.fenestros.loc

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10 <<>> centos7.fenestros.loc
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37543
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;centos7.fenestros.loc.         IN      A
```

```
;; ANSWER SECTION:
centos7.fenestros.loc.  259200  IN      A       10.0.2.51

;; AUTHORITY SECTION:
fenestros.loc.          259200  IN      NS      centos7.fenestros.loc.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 01 17:44:08 CET 2022
;; MSG SIZE  rcvd: 80
```

```
[root@centos7 ~]# dig -x 10.0.2.51

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10 <<>> -x 10.0.2.51
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48473
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;51.2.0.10.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
51.2.0.10.in-addr.arpa. 259200  IN      PTR     centos7.fenestros.loc.

;; AUTHORITY SECTION:
2.0.10.in-addr.arpa.    259200  IN      NS      centos7.fenestros.loc.

;; ADDITIONAL SECTION:
centos7.fenestros.loc.  259200  IN      A       10.0.2.51

;; Query time: 0 msec
```

```
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Nov 01 17:45:05 CET 2022
;; MSG SIZE  rcvd: 116
```

Important - Notez l'utilisation de l'option **-x** de la commande **dig** pour tester la zone à l'envers.

```
[root@centos7 ~]# host ittraining.team
ittraining.team has address 109.228.56.52
ittraining.team mail is handled by 10 aspmx3.googlemail.com.
ittraining.team mail is handled by 5 alt2.aspmx.l.google.com.
ittraining.team mail is handled by 5 aspmx.l.google.com.
ittraining.team mail is handled by 10 mx.zoho.com.
ittraining.team mail is handled by 10 aspmx2.googlemail.com.
ittraining.team mail is handled by 1 alt1.aspmx.l.google.com.
```

LAB #3 - L'utilitaire rndc

L'utilitaire de bind **rndc** est utilisé pour contrôler **named** à partir de la ligne de commande du localhost ou bien d'un hôte distant. Pour des raisons de sécurité une clef partagée doit être référencée dans le fichier de configuration de bind, **/etc/named.conf**, ainsi que dans le fichier de configuration de **rndc**, **/etc/rndc.conf**.

3.1 - La clef rndc

Premièrement il convient de créer la clef partagée :

```
[root@centos7 ~]# rndc-confgen -a -c /root/rndc.key
wrote key file "/root/rndc.key"
```

A l'examen de la clef, vous pouvez constater que son nom est **rndc-key** et que l'algorithme est **hmac-md5** :

```
[root@centos7 ~]# cat /root/rndc.key
key "rndc-key" {
        algorithm hmac-md5;
        secret "F5/TtDX+IxSbyGNNAnR48Q==";
};
```

Important - Notez le format de ce fichier.

3.2 - Les fichiers de configuration

La clef doit être référencée dans le fichier **/etc/named.conf** :

```
[root@centos7 ~]# vi /etc/named.conf
[root@centos7 ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
```

```
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query {
                localhost;
                10.0.2.0/24;
        };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};
```

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

key "rndc-key" {
        algorithm hmac-md5;
        secret "F5/TtDX+IxSbyGNNAnR48Q==";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Afin de dire à named d'écouter sur le port par défaut 953 pour des connexions en provenance de rndc, il est nécessaire d'utiliser une clause **controls** dans le fichier /etc/named.conf :

```
[root@centos7 ~]# vi /etc/named.conf
[root@centos7 ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
```

```
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query {
                localhost;
                10.0.2.0/24;
        };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";
```

```
        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

controls {
  inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};

key "rndc-key" {
        algorithm hmac-md5;
        secret "F5/TtDX+IxSbyGNNAnR48Q==";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

A ce stade, rndc ne peut pas se connecter à named. La raison est le manque du fichier **/etc/rndc.conf** :

```
[root@centos7 ~]# cat /etc/rndc.conf
```

```
cat: /etc/rndc.conf: No such file or directory
```

Créez donc ce fichier :

```
[root@centos7 ~]# vi /etc/rndc.conf
[root@centos7 ~]# cat /etc/rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "F5/TtDX+IxSbyGNNAnR48Q==";
};

options {
  default-server  localhost;
  default-key     "rndc-key";
};
```

Important - Notez la présence de la section concernant la valeur de la clef et la section qui définit le serveur par défaut et la clef par défaut. Dans le cas où vous avez plusieurs serveurs à gérer à partir d'une seule instance de rndc vous pouvez inclure des clauses supplémentaires correspondantes à chaque configuration des fichiers /etc/named.conf.

Pour prendre en compte cette configuration, re-démarrez le service named :

```
[root@centos7 ~]# systemctl restart named

[root@centos7 ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-11-02 05:47:10 CET; 8s ago
  Process: 9129 ExecStop=/bin/sh -c /usr/sbin/rndc stop > /dev/null 2>&1 || /bin/kill -TERM $MAINPID
(code=exited, status=0/SUCCESS)
```

```
  Process: 9142 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 9140 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-
checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 9144 (named)
   CGroup: /system.slice/named.service
           └─9144 /usr/sbin/named -u named -c /etc/named.conf

Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './DNSKEY/IN':
2001:500:9f::42#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './DNSKEY/IN': 2001:500:2d::d#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './DNSKEY/IN': 2001:dc3::35#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './NS/IN': 2001:dc3::35#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './DNSKEY/IN':
2001:500:200::b#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: network unreachable resolving './NS/IN': 2001:500:200::b#53
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: managed-keys-zone: Key 20326 for zone . acceptance timer
complete: key now trusted
Nov 02 05:47:10 centos7.fenestros.loc named[9144]: resolver priming query complete
```

Constatez ensuite que rndc fonctionne :

```
[root@centos7 ~]# rndc status
WARNING: key file (/etc/rndc.key) exists, but using default configuration file (/etc/rndc.conf)
version: BIND 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10 (Extended Support Version) <id:7107deb>
running on centos7.fenestros.loc: Linux x86_64 3.10.0-1160.6.1.el7.x86_64 #1 SMP Tue Nov 17 13:59:11 UTC 2020
boot time: Wed, 02 Nov 2022 04:47:10 GMT
last configured: Wed, 02 Nov 2022 04:47:10 GMT
configuration file: /etc/named.conf
CPUs found: 1
worker threads: 1
UDP listeners per interface: 1
number of zones: 105 (97 automatic)
```

```
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/900/1000
tcp clients: 2/150
server is up and running
```

Les options de cette commande sont :

```
[root@centos7 ~]# rndc --help
rndc: invalid argument --
Usage: rndc [-b address] [-c config] [-s server] [-p port]
        [-k key-file ] [-y key] [-r] [-V] command

command is one of the following:

  addzone zone [class [view]] { zone-options }
                Add zone to given view. Requires allow-new-zones option.
  delzone [-clean] zone [class [view]]
                Removes zone from given view.
  dnstap -reopen
                Close, truncate and re-open the DNSTAP output file.
  dnstap -roll count
                Close, rename and re-open the DNSTAP output file(s).
  dumpdb [-all|-cache|-zones|-adb|-bad|-fail] [view ...]
                Dump cache(s) to the dump file (named_dump.db).
  flush         Flushes all of the server's caches.
  flush [view]  Flushes the server's cache for a view.
  flushname name [view]
                Flush the given name from the server's cache(s)
  flushtree name [view]
                Flush all names under the given name from the server's cache(s)
```

```
freeze        Suspend updates to all dynamic zones.
freeze zone [class [view]]
              Suspend updates to a dynamic zone.
halt          Stop the server without saving pending updates.
halt -p       Stop the server without saving pending updates reporting
              process id.
loadkeys zone [class [view]]
              Update keys without signing immediately.
managed-keys refresh [class [view]]
              Check trust anchor for RFC 5011 key changes
managed-keys status [class [view]]
              Display RFC 5011 managed keys information
managed-keys sync [class [view]]
              Write RFC 5011 managed keys to disk
modzone zone [class [view]] { zone-options }
              Modify a zone's configuration.
              Requires allow-new-zones option.
notify zone [class [view]]
              Resend NOTIFY messages for the zone.
notrace       Set debugging level to 0.
nta -dump
              List all negative trust anchors.
nta [-lifetime duration] [-force] domain [view]
              Set a negative trust anchor, disabling DNSSEC validation
              for the given domain.
              Using -lifetime specifies the duration of the NTA, up
              to one week.
              Using -force prevents the NTA from expiring before its
              full lifetime, even if the domain can validate sooner.
nta -remove domain [view]
              Remove a negative trust anchor, re-enabling validation
              for the given domain.
querylog [ on | off ]
              Enable / disable query logging.
```

```
reconfig      Reload configuration file and new zones only.
recursing     Dump the queries that are currently recursing (named.recursing)
refresh zone [class [view]]
              Schedule immediate maintenance for a zone.
reload        Reload configuration file and zones.
reload zone [class [view]]
              Reload a single zone.
retransfer zone [class [view]]
              Retransfer a single zone without checking serial number.
scan          Scan available network interfaces for changes.
secroots [view ...]
              Write security roots to the secroots file.
showzone zone [class [view]]
              Print a zone's configuration.
sign zone [class [view]]
              Update zone keys, and sign as needed.
signing -clear all zone [class [view]]
              Remove the private records for all keys that have
              finished signing the given zone.
signing -clear <keyid>/<algorithm> zone [class [view]]
              Remove the private record that indicating the given key
              has finished signing the given zone.
signing -list zone [class [view]]
              List the private records showing the state of DNSSEC
              signing in the given zone.
signing -nsec3param hash flags iterations salt zone [class [view]]
              Add NSEC3 chain to zone if already signed.
              Prime zone with NSEC3 chain if not yet signed.
signing -nsec3param none zone [class [view]]
              Remove NSEC3 chains from zone.
signing -serial <value> zone [class [view]]
              Set the zones's serial to <value>.
stats         Write server statistics to the statistics file.
status        Display status of the server.
```

```
  stop          Save pending updates to master files and stop the server.
  stop -p       Save pending updates to master files and stop the server
                reporting process id.
  sync [-clean] Dump changes to all dynamic zones to disk, and optionally
                remove their journal files.
  sync [-clean] zone [class [view]]
                Dump a single zone's changes to disk, and optionally
                remove its journal file.
  thaw          Enable updates to all dynamic zones and reload them.
  thaw zone [class [view]]
                Enable updates to a frozen dynamic zone and reload it.
  trace         Increment debugging level by one.
  trace level   Change the debugging level.
  tsig-delete keyname [view]
                Delete a TKEY-negotiated TSIG key.
  tsig-list     List all currently active TSIG keys, including both statically
                configured and TKEY-negotiated keys.
  validation [ yes | no | status ] [view]
                Enable / disable DNSSEC validation.
  zonestatus zone [class [view]]
                Display the current status of a zone.

Version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.10
```

Important - Notez la sous-commande **reload** qui permet de recharger la configuration d'une zone spécifique sans recharger la configuration de toutes les zones.

Caractéristiques avancées de Bind

DNSSEC

DNSSEC — Abréviation de DNS SECurity, cette fonctionnalité permet aux zones d'être signées de manière cryptographique avec une clé de zone :

- De cette manière, les informations sur une zone spécifique peuvent être vérifiées comme provenant d'un serveur de noms qui l'a signée avec une clé privée particulière, tant que le destinataire possède la clé publique de ce serveur de noms.

BIND version 9 prend également en charge la méthode d'authentification des messages par clé publique/privée SIG(0).

TSIG

TSIG — Abréviation de Transaction SIGNatures, cette fonctionnalité permet un transfert du maître vers l'esclave uniquement après avoir vérifié qu'une clé secrète partagée existe sur les deux serveurs de noms :

- Cette fonctionnalité renforce la méthode standard d'autorisation de transfert basée sur l'adresse IP. Un attaquant aurait non seulement besoin d'avoir accès à l'adresse IP pour transférer la zone, mais il aurait également besoin de connaître la clé secrète.

BIND version 9 prend également en charge TKEY, qui est une autre méthode de clé secrète partagée pour autoriser les transferts de zone.
